UNITED STATES DISTRICT COURT
FOR THE
DISTRICT OF VERMONT

UNITED STATES OF AMERICA,	)	
	)	
v.	)	Case No. 2:18-cr-00026
	)	
COLIN GERMAIN	)	

OPINION AND ORDER
DENYING DEFENDANT'S MOTION TO SUPPRESS
(Doc. 41)

Defendant Colin Germain is charged in a two-count Indictment alleging he knowingly transported child pornography in, or affecting, interstate or foreign commerce by any means, including by computer in violation of 18 U.S.C. §§ 2252A(a)(1) and 2252A(b)(1), and "forcibly assaulted, opposed, impeded, and interfered with" a Special Agent of the United States while the Special Agent was engaged in the performance of official duties in violation of 18 U.S.C. § 111(a)(1). (Doc. 20.) On September 4, 2018, Defendant filed a motion to suppress (Doc. 41), contending that his personal information was improperly subpoenaed from Waitsfield Telecom and Google in violation of the Fourth Amendment to the United States Constitution. He seeks suppression of all evidence obtained via the subpoenas and related search warrants.[1] On October 2, 2018, the government opposed the motion. The parties waived a hearing on April 11, 2019, at which time the court took the pending motion under advisement.

Defendant is represented by Assistant Federal Public Defender Elizabeth K. Quinn. The government is represented by Assistant United States Attorney Nicole P. Cate.

[1] Defendant also moves to suppress evidence obtained as a result of law enforcement's search of his notebooks. This issue is moot because the government has stated it will not introduce any evidence obtained from the search of Defendant's notebooks in its case-in-chief.

I. Findings of Fact.

Because the parties waived an evidentiary hearing, the following facts are derived from the parties' briefing. In August 2017, agents from Homeland Security Investigations ("HSI") arrested an individual in Tennessee for child pornography offenses. This individual consented to searches of multiple online accounts including an email account in which law enforcement found an email dated August 2, 2017, which the offender received from "daddylittlekitty12@gmail.com" with no text in the body of the email but with a video attachment containing child pornography.

On September 8, 2017, Tennessee HSI obtained a federal search warrant for the "daddylittlekitty12@gmail.com" account. In response to that search warrant, Google produced account records including IP addresses associated with the email account. Tennessee HSI determined that an IP address associated with the "daddylittlekitty12@gmail.com" account was provided by Waitsfield Telecom, an internet service company in Vermont.

After communicating with Vermont HSI, Tennessee HSI sent a summons to Waitsfield Telecom requesting all records regarding the identity of the customer associated with the IP address, including registrant name, address, associated email addresses, all MAC addresses, telephone number, status of account, available IP history, length of service, and the date account was opened. In response, on October 5, 2017, Waitsfield Telecom identified the subscribers as Wade and Maureen Stevens, Defendant's stepfather and mother, at 724 Twitchell Road, New Haven, VT 05472, provided their telephone number, and indicated that their IP address had been continuously held from June 22, 2017 to September 20, 2017.

Google's response to the search warrant included not only a copy of the August 2, 2017 email from "daddylittlekitty12@gmail.com" but also an email dated August 3, 2017 with an attached photo of a male's genitals and text which indicated that the photo was of the account owner. HSI investigators in Vermont determined that the GPS coordinates associated with the photo attachment corresponded with the residence at 724 Twitchell Road in New Haven, Vermont. Law enforcement thereafter conducted surveillance of

the property and were able to confirm that the vehicles parked in the residence's driveway were registered to Wade Stevens.

HSI investigators in Vermont subsequently obtained a search warrant for the 724 Twitchell Road property. On November 7, 2017, law enforcement agents executed the search warrant, conducted the search, and took Defendant into custody. After his arrest, Defendant waived his *Miranda* rights and made certain incriminating statements.

In the course of their investigation, law enforcement identified four additional Google email addresses associated with Defendant. Three of the addresses, "mommylovesyounggirls@gmail.com," "spankmedaddy10@gmail.com," and "stormmodz1997@gmail.com," were identified based on records from the "daddylittlekitty12@gmail.com" account. The fourth Google email address was identified from an iPod touch seized during the November 7, 2017 search, which had the owner name "Kitty Playtime" and the associated Apple ID "pitbulletmods@gmail.com." On February 16, 2018, grand jury subpoenas were served on Google for account information related to the four email accounts.

In response to the grand jury subpoenas, Google produced subscriber information including subscriber name, recovery email address,[2] account creation date, and IP addresses associated with login dates and times. The recovery email address for the "pitbulletmods@gmail.com" account identified a fifth Google email address, "stevenscolinbenny11@gmail.com," associated with Defendant.[3]

On April 20, 2018, HSI obtained a federal search warrant for the five Google accounts law enforcement believed were associated with Defendant. Examination of the data Google provided from several of those accounts revealed additional files allegedly containing child pornography.

---

[2] If an account has a recovery email address, Google can use that email address to assist user access to the account or alert the user to any unusual account activity.

[3] No subpoena was issued for this account. Defendant's middle name is Benjamin.

II. Conclusions of Law and Analysis.

Defendant asserts the government obtained records from Waitsfield Telecom and Google without a search warrant and thereby violated his reasonable expectation of privacy in account information in violation of the Fourth Amendment. He relies on *Carpenter v. United States*, 138 S. Ct. 2206 (2018), for his argument and contends that the third-party disclosure doctrine is not "a hard and fast rule and is instead simply one factor in the overall-reasonable-expectation-of-privacy analysis." (Doc. 41 at 12.) The government responds that no Fourth Amendment violation occurred because Defendant does not have a reasonable expectation of privacy in business records maintained by a third party.

The Fourth Amendment to the United States Constitution provides that:

> [t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. CONST. amend. IV. "[A] Fourth Amendment search occurs when the government violates a subjective expectation of privacy that society recognizes as reasonable." *Kyllo v. United States*, 533 U.S. 27, 33 (2001).

The third-party doctrine recognizes that "[a] person has no legitimate expectation of privacy in information he voluntarily turns over to third parties[.]" *Smith v. Maryland*, 442 U.S. 735, 743-44 (1979); *see also Katz v. United States*, 389 U.S. 347, 351 ("[T]he Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."); *United States v. Davis*, 785 F.3d 498, 507 (11th Cir. 2015) ("*Katz* posits a two-part inquiry: first, has the individual manifested a subjective expectation of privacy in the object of the challenged search . . . [and] is society willing to recognize that expectation as reasonable? [The] party alleging an unconstitutional search . . . must establish both a subjective and an objective expectation of privacy[.]") (citations, internal quotation marks, and emphasis omitted).

In *Carpenter v. United States*, the Supreme Court held that cell-site location information ("CSLI") was not subject to the third-party doctrine because "the notion that an individual has a reduced expectation of privacy in information knowingly shared with another" or that an individual has engaged in "voluntary exposure" by his or her mere physical movements and use of a cell phone extends the doctrine too far. 138 S. Ct. at 2219-20. As a result, "[w]hether the Government employs its own surveillance technology . . . or leverages the technology of a wireless carrier, . . . an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI." *Id.* at 2217. In so ruling, the Court focused on the "special solicitude for location information" which protects individuals from warrantless searches of "detailed chronicle[s]" of their movements. *Id.* at 2219-20. The Court described its decision in *Carpenter* as a "narrow" one that "[did] not disturb the application of *Smith* [*v. Maryland*, 442 U.S. 735 (1979)] and [*United States v.*] *Miller*[, 425 U.S. 435 (1976),] or call into question conventional surveillance techniques and tools, such as security cameras. Nor [does it] address other business records that might incidentally reveal location information." *Id.* at 2220.

Since *Carpenter*, courts have held that IP addresses and related information remain "comfortably within the scope of the third-party doctrine" because such information "had no bearing on any person's day-to-day movement" and an individual "lacked a reasonable expectation of privacy in that information." *United States v. Contreras*, 905 F.3d 853, 857 (5th Cir. 2018). "The privacy interest in this type of identifying data, which presumably any [internet provider] employee could access during the regular course of business, simply does not rise to the level of the evidence in *Carpenter* such that it would require law enforcement to obtain a search warrant." *United States v. Tolbert*, 326 F. Supp. 3d 1211, 1225 (D.N.M. 2018); *see also United States v. Felton*, 2019 WL 659238, at *2 (W.D. La. Feb. 15, 2019) ("The Court finds that the subpoena issued in this case was issued to obtain third-party business records and thus, Felton had a reduced expectation of privacy."); *United States v. Rosenow*, 2018 WL 6064949, at *11 (S.D. Cal. Nov. 20, 2018) ("The Court concludes that Defendant had no

reasonable expectation of privacy in the subscriber information and the IP log-in information Defendant voluntarily provided to the online service providers in order to establish and maintain his account.").

In this case, law enforcement obtained information from Waitsfield Telecom and Google who maintained that data as part of their provision of internet services. The information at issue does not reveal Defendant's physical movements or the location of his cell phone. Instead, it consists of account information in which Defendant has no reasonable expectation of privacy. Accordingly, no Fourth Amendment violation occurred. *See United States v. Wheelock*, 772 F.3d 825, 828-29 (8th Cir. 2014) (holding third-party disclosure doctrine is "dispositive" because a defendant "cannot claim a reasonable expectation of privacy in the government's acquisition of his subscriber information, including his IP address and name from third-party service providers.") (alteration and internal quotation marks omitted).

CONCLUSION

For the reasons stated above, Defendant's motion to suppress is DENIED. (Doc. 41.)

SO ORDERED.

Dated at Burlington, in the District of Vermont, this 3rd day of May, 2019.

Christina Reiss, District Judge
United States District Court